Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
wojciech.trabka@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

WARUNKI WPROWADZENIA POWSZECHNEGO SYSTEMU IDENTYFIKACJI ELEKTRONICZNEJ I UWIERZYTELNIANIA W SYSTEMIE INFORMACYJNYM OPIEKI ZDROWOTNEJ

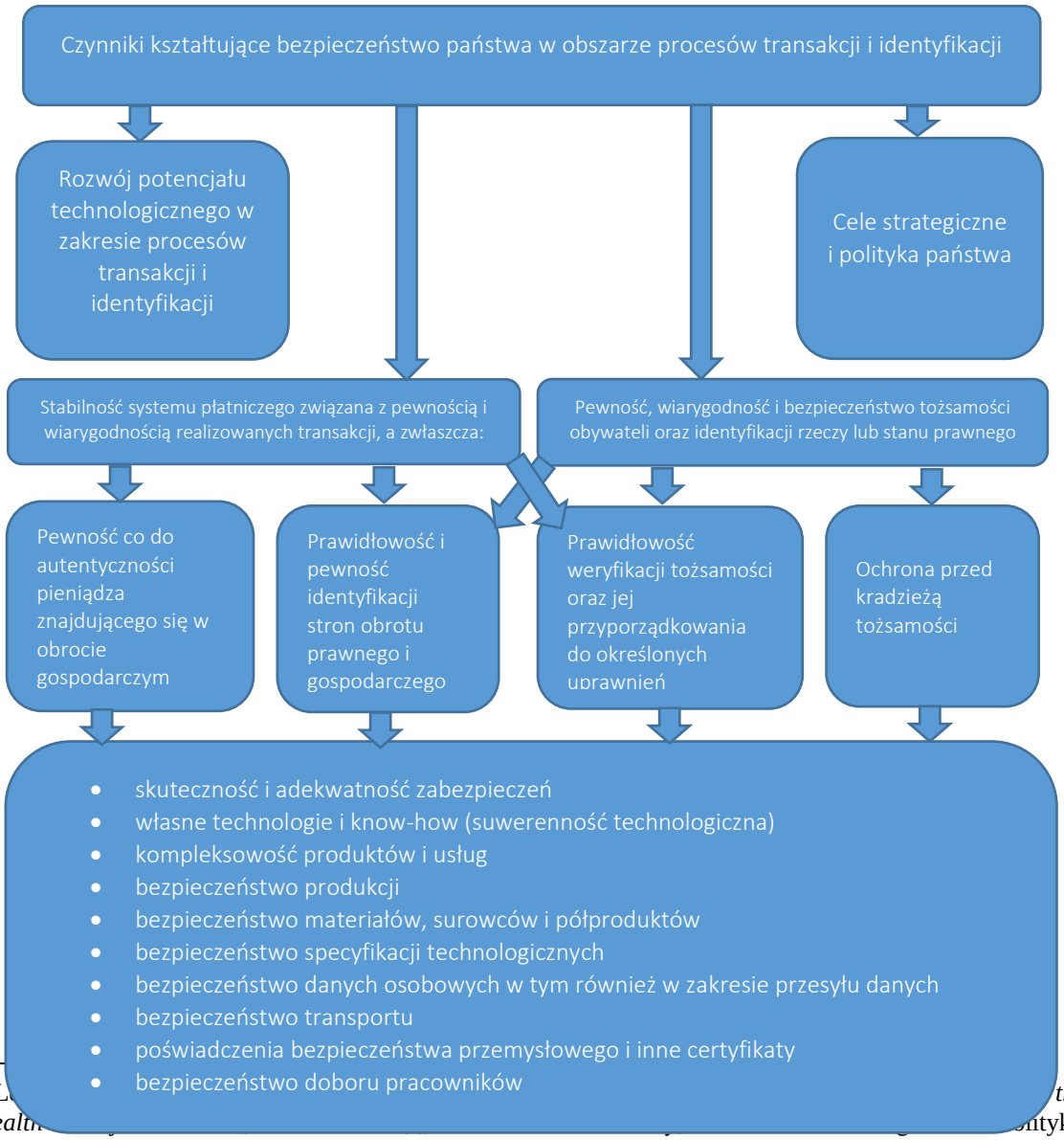
Wstęp

Zastosowanie nowoczesnych technologii teleinformatycznych w systemie informacyjnym administracji publicznej w Polsce należy postrzegać jako milowy krok w kierunku budowania infrastruktury umożliwiającej udostępnianie usług identyfikacji elektronicznej i uwierzytelnienia także w systemie opieki zdrowotnej. Jak w każdym przypadku funkcjonowania systemu informacyjnego przetwarzającego informacje w oparciu o dokumentację elektroniczną oraz zaawansowane rozwiązania służące weryfikacji tożsamości poszczególnych kategorii użytkowników dysponujących określonym, przydzielonym dostępem do zasobów cyfrowych takiego systemu, o szczególnym znaczeniu dla sprawnego zarządzania takim systemem jest zagwarantowanie wszystkim jego uczestnikom tzw. bezpieczeństwa identyfikacyjnego. Termin ten oznacza stan niezakłóconego bezpieczeństwa państwa w obszarze obejmującym 1) prawidłową weryfikację deklarowanej tożsamości osób,

2) weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się posługuje, 3) obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość lub określone uprawnienia, a także 4) ochronę obywateli przed kradzieżą tożsamości[1] – patrz. Rys. 1.

Pierwsze próby zastosowania rozwiązań teleinformatycznych mających na celu zapewnienie bezpieczeństwa identyfikacyjnego w polskim systemie opieki zdrowotnej poprzez weryfikację statusu ubezpieczeniowego pacjenta oraz autoryzację zrealizowanych świadczeń zostały podjęte w 2001 roku w województwie śląskim wraz z uruchomieniem lokalnego systemu tzw. elektronicznej karty ubezpieczenia zdrowotnego.

Rys. 1. Uwarunkowania bezpieczeństwa państwa w kontekście wiarygodności identyfikacji



[1] L… *the health*… …lityka Zdrowotna" 2015, nr 16, s. 77

Źródło: Lewandowski R., *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów* w: Goc. M., Tomaszewski T., Lewandowski R., *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Volumina, Warszawa 2016, s. 289

Umożliwiała ona przede wszystkim weryfikację w systemie śląskiego oddziału płatnika zdrowotnego (ówczesnej Kasy Chorych, obecnie Narodowego Funduszu Zdrowia) statusu ubezpieczeniowego użytkownika karty oraz autoryzację wykonanych świadczeń w ramach realizacji kontraktu ze śląskim oddziałem płatnika. Za pomocą karty lekarze mieli również możliwość wydruku recept, zaś placówki zdrowotne mogły prowadzić racjonalną gospodarkę lekami za pomocą przetwarzanych danych dotyczących wystawionych recept. Takie rozwiązanie pozwalało na „uszczelnienie" obrotu farmaceutykami oraz szybsze wykrycie ewentualnych nieprawidłowości w tym zakresie[2].

W 2007 roku zaprezentowano koncepcję ówczesnego prezesa Narodowego Funduszu Zdrowia według której miały zostać wprowadzone bony zdrowotne o określonej wartości, które miały zaktywizować rynek ubezpieczeń zdrowotnych i przynieść oszczędności na kosztach administracyjnych ponoszonych przez Zakład Ubezpieczeń Społecznych. Pomysł ten nie został jednak wprowadzony w życie[3].

Od 2013 roku w Polsce rozpoczął działalność system elektronicznej weryfikacji uprawnień świadczeniobiorców (eWUŚ), dzięki któremu istnieje możliwość natychmiastowego (w czasie rzeczywistym) potwierdzenia prawa pacjenta do świadczeń opieki zdrowotnej finansowanych ze środków publicznych. Aplikacja znacząco uprościła i przyśpieszyła weryfikację statusu ubezpieczeniowego pacjentów przez świadczeniodawcę zastępując konieczność posiadania dotychczasowych druków RMUA lub legitymacji emeryta/rencisty[4]. W poszukiwaniu jeszcze bardziej funkcjonalnych rozwiązań teleinformatycznych wychodzących naprzeciw wymaganiom i uwarunkowaniom współczesnego systemu opieki zdrowotnej dokonano rewizji dotychczas stosowanych środków identyfikacji w sektorze zdrowia. Do słabych stron modelu śląskiej karty ubezpieczenia

[2] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany. Źródło internetowe: https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, data dostępu: 09.05.2017

[3] Tamże

[4] Tamże

zdrowotnego jedynie lokalny charakter aplikacji i dość ograniczoną funkcjonalność takiego nośnika informacyjnego.

Odpowiedzią na powyższe wnioski była zaproponowana w 2015 roku koncepcja rządowa zakładająca uruchomienie trzech rodzajów kart elektronicznych i powiązanych z nimi systemów teleinformatycznych w systemie ochrony zdrowia, tj. 1) Karty Ubezpieczenia Zdrowotnego (KUZ), 2) Karty Specjalisty Medycznego (KSM) oraz 3) Karty Specjalisty Administracyjnego (KSA). W początkowym założeniu nowe rodzaje nośników oraz zarządzające nimi systemy informatyczne miały zostać objęte regulacjami zawartymi w projektowanej nowelizacji ustawy z 29 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Jednak z biegiem czasu inicjatywa rządowa została zarzucona przez samego pomysłodawcę z uwagi na dostrzegane problemy legislacyjne i mankamenty techniczne proponowanej koncepcji stawiające pod znakiem zapytania kwestię zapewnienia bezpieczeństwa identyfikacyjnego pacjentów.

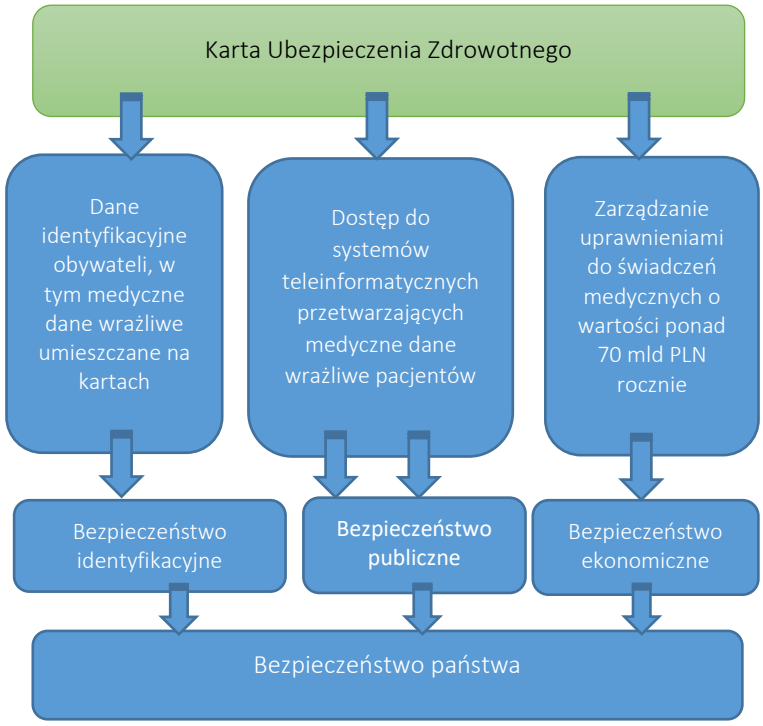
Aktualnie obserwuje się powrót do pierwotnej koncepcji Elektronicznej Karty Ubezpieczenia Zdrowotnego (e-KUZ), która miałaby zostać wprowadzona jako ulepszona wersja poprzedniego projektu i uwzględniać zmiany korygujące ograniczenia wcześniejszej koncepcji. Z uwagi na kluczową rolę e-KUZ jako dokumentu publicznego o strategicznym znaczeniu dla bezpieczeństwa identyfikacyjnego i uwierzytelniania obywateli jej szczegółowa specyfikacja techniczna i zastosowane rozwiązania informatyczne powinny spełniać wymóg szczególnego nadzoru regulacyjnego ze strony projektodawcy[5] – patrz. Rys. 2. Kwestią decyzji pozostaje wybór docelowej formy funkcjonowania e-KUZ spełniającej ustawowy wymóg powszechności. W chwili obecnej rozważane są co najmniej dwa możliwe warianty wyboru, tj. wydawanie eKUZ jako odrębnego dokumentu publicznego lub włączenie funkcjonalności e-KUZ w inny, powszechny dokumenty publiczny (czyli elektroniczny dowód osobisty, który jako jedyny dokument publiczny spełnia wymóg powszechności)[6]. Kontrowersje budzi natomiast propozycja połączenia Elektronicznej Karty Ubezpieczenia Zdrowotnego z kartą płatniczą wydawaną przez banki jako sprzeczna z zaprezentowaną 2015 roku przez Ministra Cyfryzacji strategiczną koncepcją wykorzystania elektronicznego dowodu osobistego w roli

[5] Lewandowski R, Miękina A. *Certyfikacja w zakresie Common Criteria – wstępna koncepcja budowy polskiego modelu*. Człowiek i Dokumenty. 2015;39:35.

[6] Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, Polski Przegląd Nauk o Zdrowiu 3;(48): 2016

uniwersalnego i powszechnego narzędzia identyfikacyjnego, który miałby zastąpić innego rodzaju karty dostępu do usług identyfikacji i uwierzytelnienia[7].

Rys. 2. Model KUZ w kontekście bezpieczeństwa państwa



Źródło: Lewandowski R. *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA.* Journal of Health Policy, Insurance and Management – Polityka Zdrowotna. 2015;16:75–84 w: Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego,* Polski Przegląd Nauk o Zdrowiu 3;(48): 2016

Identyfikacja elektroniczna w świetle wybranych rozwiązań europejskich

W ubiegłym roku weszło w życie Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE L z dn. 28 sierpnia 2014 r.) znane szerzej pod nazwą eIDAS[8]. Powyższy dokument prawny obowiązuje na terenie Unii Europejskiej w sposób bezpośredni i nie wymagający implementacji do prawa krajowego poszczególnych państw członkowskich. Mimo tej generalnej zasady w kilku obszarach

[7] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany. Źródło internetowe: https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, data dostępu: 09.05.2017

[8] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910

regulowanych przez eIDAS pozostawiono swobodę dla ustawodawcy krajowego, stąd też w naszym kraju przygotowana została ustawa o usługach zaufania, identyfikacji elektronicznej oraz zmiany niektórych ustaw[9]. Rozporządzenie eIDAS zasadniczo tworzy regulacyjne ramy dla zapewnienie wzajemnego uznawania środków elektronicznej identyfikacji i uwierzytelniania umożliwiając tym samym rzeczywiste funkcjonowanie transgranicznej opieki zdrowotnej dla obywateli Europy.

Ilustracją dla dobrych praktyk realizowanych w celu adaptacji systemu legislacyjnego oraz organizacyjnego względem regulacji rozporządzenia eIDAS może być Austria. Koordynacją obydwu procesów zajmuje się odpowiedzialny za informatyzację państwa Urząd Kanclerza Austrii we współpracy z Ministerstwem Sprawiedliwości (w zakresie prac legislacyjnych). Punktem wyjścia do rozpoczęcia harmonizacji było przygotowanie przez Austrię otwartej specyfikacji API określanej mianem „warstwy bezpieczeństwa" na użytek składania podpisów za pomocą urządzenia mobilnego lub karty obywatelskiej. Jednym z rozwiązań zaprojektowanych w oparciu o powyższą specyfikację jest dostępna nieodpłatnie dla osób fizycznych i przedsiębiorców implementacja MOCCA. Bazuje ona na licencji *open-source* i została opracowana we współpracy Urzędu Kanclerskiego i Politechniki w Grazu. Dostępne są też trzy inne aplikacje, które można znaleźć na dedykowanym portalu internetowym[10]. Specyfikacja API umożliwia sprawne integrowanie rozwiązań w innych aplikacjach (np. systemach typu *workflow*). Dostępne są również aplikacje do składania podpisów w formacie PDF[11]. Rozwiązania austriackie uczestniczyły w testach prowadzonych przez Europejski Instytut Norm Telekomunikacyjnych (*European Telecommunications Standards Institute,* ETSI) uzyskując rozpoznawalność austriackich podpisów w innych państwach członkowskich. W celu zachowania kompatybilności wstecznej ze starszymi podpisami nadal jednak funkcjonuje dedykowany portal internetowy[12].

Uzupełnienie do regulacji eIDAS w zakresie przyjętych zasad identyfikacji elektronicznej i uwierzytelnienia stanowi wypracowany w ramach projektu STORK (*Secure Identity Across Borders Linked)* model interoperacyjności w odniesieniu do stosowanych już

[9] https://legislacja.rcl.gov.pl/projekt/12283556, Projekt ustawy o usługach zaufania, identyfikacji elektronicznej oraz zmianie niektórych ustaw

[10] Źródło internetowe: https://www.buergerkarte.at/en/downloads-card.html, data dostępu: 19.05.2017

[11] Źródło internetowe: https://www.buergerkarte.at/en/pdf-signature-mobile.html, data dostępu: 19.05.2017

[12] Źródło internetowe: www.signature-verification.gv.at, data dostępu: 19.05.2017

rozwiązań w obszarze e-identyfikacji obowiązujących w krajach członkowskich[13]. Podobnie, jak w przypadku eIDAS celem projektu STORK było wypracowanie uniwersalnych metod transgranicznego uwierzytelnienia i identyfikacji obywatela. W ramach projektu powstał tzw. federacyjny model uwierzytelnienia i identyfikacji PEPS (*Pan-European Proxy Services* – Paneuropejskie Usługi Pośredniczące) oraz rozwiązania wykorzystujące nośniki kryptograficzne stanowiące źródło informacji na temat tożsamości obywatela (model *middleware*). Takie rozwiązanie ma umożliwić funkcjonowanie jednolitego europejskiego obszaru elektronicznej identyfikacji i uwierzytelnienia zapewniającego rzeczywistą interoperacyjność na poziomie krajowym oraz unijnym dla dowodów tożsamości elektronicznej (zarówno dla osób prawnych, jak i fizycznych).

Istota działania wypracowanego modelu jest stosunkowo prosta: zgłoszenie użytkownika chcącego skorzystać z systemu identyfikacji elektronicznej i uwierzytelnienia za pomocą jego przeglądarki internetowej przekierowywane jest do centrum krajowych usług uwierzytelniających, gdzie za pomocą uwierzytelnienia potwierdzana jest tożsamość użytkownika. Uwierzytelnione w ten sposób dane identyfikacyjne mogą być następnie przekazane do wybranego przez użytkownika usługodawcy[14]. Z kolei w komplementarnym modelu *middleware* proces uwierzytelnienia i odczytu danych identyfikacyjnych dokonuje się z wykorzystaniem nośnika kryptograficznego za pośrednictwem oprogramowania *middleware* zainstalowanego na stacji użytkownika. Komunikacja z usługami PEPS odbywa się tu poprzez tzw. wirtualnego dostawcę tożsamości (V-IDP). W obydwu powyższych przypadkach uwierzytelnione dane są przekazywane do usługodawcy[15].

W poszukiwaniu efektywnych rozwiązań regulujących publiczny schemat identyfikacji elektronicznej i usług zaufania w Polsce interesujących wniosków dostarcza analiza porównawcza takich schematów funkcjonujących w Austrii oraz Szwecji. W przypadku Austrii scentralizowany i zamknięty system uniemożliwia prywatnym podmiotom pełnienia funkcji udostępniania tożsamości. Mogę one jedynie wydawać określone nośniki tożsamości. Z kolei państwo bierze na siebie ciężar zapewnienia kompletnej infrastruktury ponosząc ciężar koniecznych inwestycji i jej utrzymania. Co istotne, usługi dostarczane w ramach austriackiego systemu są darmowe dla obywateli, a państwo obok usług identyfikacji i uwierzytelnienia,

[13] https://www.eid-stork.eu
[14] Wachnik D., *Rozporządzenie eIDAS - na pograniczu technologii i prawa*. Elektronika 2/2014: 42-44

[15] Tamże

dostarcza także usługę podpisu elektronicznego. Z technicznego punktu widzenia zaplecze infrastrukturalne austriackiego systemu oraz obowiązujący w nim model integracji z dostawcami usług zaufania można określić jako mechanizmy skomplikowane, a nawet w części odbiegające od obecnych standardów światowych funkcjonujących w tym obszarze. Jednakże takie podejście wynika przede wszystkim ze specyficznych i restrykcyjnych uregulowań prawnych w zakresie identyfikacji obywateli (w tym kwestii ochrony prywatności). Co ciekawe, nawet w tak zorganizowanym systemie, w którym praktycznie każdy obywatel posiada możliwość identyfikacji elektronicznej, stopień wykorzystania tej funkcjonalności nie jest wysoki (8,5 mln obywateli generuje tylko 650 tys. transakcji rocznie). Skala wykorzystywania możliwości identyfikacji elektronicznej za pomocą kart również jest dość niska. Oznaki poprawy w tym obszarze zaobserwowano dopiero po udostępnieniu takiej funkcjonalności na platformach mobilnych.

W przeciwieństwie do rozwiązań austriackich Szwecja stanowi przykład rynkowego podejścia w organizowaniu systemu elektronicznej identyfikacji obywateli. W jego funkcjonowanie zaangażowane są nie tylko firmy prywatne, od których państwa nabywa usługi identyfikacji dla cyfrowych usług publicznych - sfederalizowany model przewiduje możliwość włączenia do systemu dowolnych podmiotów gospodarczych, które spełnią określone wymagania. Takie podejście w praktyce cechuje się znaczną prostotą rozwiązań technicznych i szeroką skalą zastosowania społecznego plasując Szwecję w czołówce krajów z najlepiej rozwiniętym sektorem *e-government* oraz wysokim stopniem wykorzystania środków identyfikacji elektronicznej (9,5 mln obywateli generuje ponad 300 mln transakcji rocznie). Na podstawie powyższego porównania widać wyraźnie większą efektywność federacyjnego modelu szwedzkiego otwartego na włączanie w proces autonomicznego (tzn. pozbawionego presji wywieranej ze strony państwa) tworzenia i integracji rozwiązań technicznych firm prywatnych. Obywatele Szwecji znacznie częściej używają środków identyfikacji elektronicznej pomimo, że to w Austrii występuje większe nasycenie takimi technologiami. Rozwiązania austriackie są jednak o wiele bardziej skomplikowane, niż szwedzkie, a ich elastyczność ograniczana jest rozwojem infrastruktury centralnej. Fakt ten może mieć znaczenie w kontekście federacyjnego, a więc zbieżnego z doświadczeniami szwedzkimi,

sposobu realizacji koncepcji funkcjonowania prywatnych centrów certyfikacyjnych wydających certyfikaty (kwalifikowane) uznawane w usługach publicznych w Polsce[16].

Niezwykle użytecznym rozwiązaniem w zakresie przetwarzania dokumentów elektronicznych (np. elektronicznej dokumentacji medycznej) jest szeroko wykorzystywana m.in. w krajach skandynawskich usługa rejestrowanego doręczenia elektronicznego (ang. *electronic delivery service,* EDS lub *e-delivery*)[17]. Jest ona cyfrowym odpowiednikiem tradycyjnego listu poleconego, gdzie dokumenty są podpisywane elektroniczne przez obywateli lub firmy, a dowody ich doręczeń tworzą systemy informatyczne administracji. Zgodnie z art. 3, pkt. 36 rozporządzenia eIDAS „usługa rejestrowanego doręczenia elektronicznego" oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany. Na podstawie definicji „usług zaufania" zamieszczonej w rozporządzeniu eIDAS (artykuł 3, punkt 16) wynika, że w ramach mogą być świadczone usługi „tworzenia rejestrowanego doręczania elektronicznego" rozumiane jako tworzenie dowodów w wyniku działania usługi eIDAS, „weryfikacji rejestrowanego doręczenia elektronicznego" rozumiane jako weryfikacja certyfikatów, przy wykorzystaniu / użyciu których powstały dowody usługi rejestrowanego doręczenia elektronicznego oraz „walidacji rejestrowanego doręczenia elektronicznego" rozumiane jako walidacja dowodów elektronicznych, np. podpisów pod dowodami usługi *e-delivery*, prezentowanie daty i czasu zawartego w takim dowodzie, określenie nadawców i odbiorców w oparciu o dowody takiej usługi.

Przykładowo w Norwegii podmiot administrujący dla systemu doręczeń elektronicznych zarządza równocześnie systemem tożsamości elektronicznej, a komunikacja pomiędzy obywatelem i organami administracji publicznej odbywa się standardowo w trybie elektronicznym. Jednocześnie każdy obywatel może zdecydować o przywróceniu tradycyjnego trybu komunikacji. Z kolei w Niemczech już od 2011 roku obowiązują regulacje prawne

[16] Projekt ustawy o zmianie ustawy usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, Ministerstwo Cyfryzacji, 2017.

[17] Kawiński A., Sieradz A.[red.], *Wyzwania informatyki bankowej*: materiał przygotowany na podstawie seminariów IT w instytucjach finansowych organizowanych przez Gdańską Akademię Bankową Instytut Badań nad Gospodarką Rynkową, Gdańsk 2014

umożliwiające funkcjonowania systemu DE-Mail, który umożliwia elektroniczną wymianę wiążących prawnie dokumentów pomiędzy obywatelami, podmiotami publicznymi i prywatnymi. W tym przypadku rolą państwa pozostaje jedynie zdefiniowanie standardów technicznych i podstaw prawnych do funkcjonowania takiego systemu, bez spełniania roli dostawcy usługi.

Obecna struktura funkcjonalności krajowego systemu ePUAP umożliwia relatywnie prostą implementację usługi rejestrowanego doręczenia elektronicznego. Zakładając dopuszczenie adresu elektronicznego jako rejestrowanego adresu dla powiadomień urzędowych oraz udostępnienie skrzynki ePUAP także dla podmiotów niepublicznych proces adaptacji do standardów technicznych w kontekście rozporządzenia eIDAS może przyczynić się do znacznie bardziej powszechnego, niż dotychczas, wykorzystywania platformy ePUAP[18].

Elektroniczny dowód osobisty - uniwersalne narzędzie identyfikacji

Jednym z fundamentów cyfrowej infrastruktury administracji państwowej ma być wdrożenie systemu elektronicznych dowodów osobistych (dowodu osobistego z warstwą elektroniczną). Takie rozwiązanie ma umożliwiać m.in. powszechną identyfikację elektroniczną i uwierzytelnianie informacji dotyczących obywateli w relacjach z instytucjami administracji publicznej. Uniwersalność i kompleksowość projektowanych funkcjonalności elektronicznego dowodu osobistego umożliwi ich zastosowanie do celów identyfikacji elektronicznej także w wielu innych sektorowych systemach informacyjnych państwa, w tym w opiece zdrowotnej.

Podstawowy i powszechny dokument identyfikacyjny, jakim ma być elektroniczny dowód osobisty, zgodnie z planem działań strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych ma być wykorzystany jako platforma uwierzytelnienia w systemach teleinformatycznych oraz jako rejestr zawierający m.in. dane medyczne obywateli. Co więcej, instytucja dowodu osobistego z warstwą elektroniczną funkcjonująca obecnie w 26. państwach Europy może posiadać inne funkcjonalności zwiększające

[18] Tamże

bezpieczeństwo identyfikacyjne pacjenta, m.in. podpis elektroniczny, dokument podróży zgodny z ICAO, ew. ratunkowe dane medyczne czy biometrię[19].

Ciekawym przykładem rozwiązań w tym zakresie może być Belgia. W tym kraju zaimplementowano elektroniczne dowody osobiste umożliwiające identyfikację obywateli zarówno *online*, jak i w sposób konwencjonalny, tradycyjny. Rozwiązania belgijskie opierają się na trzech różnych typologiach dowodów osobistych przydzielanych określonym kategoriom użytkowników i umożliwiających dostęp do precyzyjnie zdefiniowanych rodzajach usług. Pierwszy rodzaj takiego dokumentu to eID czyli karta wydawana wyłącznie obywatelom belgijskim. Jej działanie przypomina funkcjonalność zwykłej karty bankomatowej z numerem PIN. Posiada mikroprocesor z zakodowanymi elektronicznie danymi identyfikacyjnymi obywatela oraz certyfikaty cyfrowe. Za jej pomocą użytkownik może potwierdzać swoją tożsamość, a tym samym swobodnie podróżować na terenie Unii Europejskiej. Dodatkowo taki elektroniczny dowód osobisty może służyć do potwierdzania tożsamości w sieci Internet, uzupełniania dokumentów i formularzy urzędowych, a także pełnić funkcję potwierdzania tożsamości użytkownika np. w bibliotece publicznej czy zaufanej sieci komputerowej. Wszystkich czynności użytkownik dokonuje wykorzystując tylko jeden podpis elektroniczny.

Drugi rodzaj elektronicznego dowodu osobistego nazywa się kids-ID. Dokument ten przysługuje osobom, które nie ukończyły 12. roku życia, a jego posiadanie nie jest obowiązkowe. Jest jednak wymagane w przypadku, gdy osoba małoletnia zamierza podróżować po terenie Unii Europejskiej. Swoją architekturą dokument kids-ID przypomina omówiony wcześniej eID. Węższy zakres uprawnień „mniejszego" elektronicznego dowodu osobistego sprzyja jego zastosowaniom w pilotażowych testach nowych funkcjonalności w zakresie np. rejestracji dzieci do szkoły czy wybranego klubu sportowego. Pozwala również na wpisanie do siedmiu numerów kontaktowych ułatwiających dotarcie do osób bezpośrednio związanych z dzieckiem w sytuacjach awaryjnych. Trzecią kategorię stanowi elektroniczny dowód osobisty wydawany obcokrajowcom zastępujący pozwolenie na pobyt cudzoziemca na terenie Belgii. Jego posiadacz uzyskuje tym samym dostęp do usług belgijskiej e-administracji oraz mieć możliwość cyfrowego podpisywania dokumentów urzędowych.

[19] Program Zintegrowanej Informatyzacji Państwa. Ministerstwo Cyfryzacji, Warszawa 2016. Źródło internetowe: https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, data dostępu: 06.05.2017

Podobnie jak w przypadku belgijskiego eID także włoskie elektroniczne dowody osobiste mają umożliwiać identyfikację obywateli w systemie *online* oraz tradycyjnym. W powszechnym użyciu są dwa rodzaje kart identyfikacyjnych umożliwiających dostęp do usług publicznych *online*: EIC ‑ tzw. opisane dowody elektroniczne oraz CNS (*Carta Nazionale dei Servizi*) czyli karty zawierające podpisy cyfrowe, które były stosowane przed wdrożeniem elektronicznych dowodów osobistych. Pierwotnie miały zostać wygaszone z końcem 2007 roku, jednak na skutek zmiany decyzji pozostają aktywne i mają być rozbudowywane o nowe funkcjonalności[20].

System identyfikacji elektronicznej i uwierzytelnienia – doświadczenia krajowe

Kluczowym warunkiem rozwoju sprawnie funkcjonującego państwa jest zapewnienie i utrzymanie wysokiego standardu przetwarzanych informacji oraz jakości usług administracji publicznej. Zastosowanie nowoczesnych rozwiązań informatycznych w tym obszarze wspiera integralność systemu informacyjnego państwa oferując jego użytkownikom dostęp do całkiem nowych funkcjonalności domeny cyfrowej. Usprawnienie procesu informatyzacji administracji publicznej było jednym z postulatów opracowanego w 2011 roku projektu Planu Informatyzacji Państwa na lata 2011-2015[21]. Na liście priorytetów zgłoszonych do realizacji znalazły się trzy główne obszary, w ramach których zamierzono skoordynować proces wdrożenia elektronicznych usług publicznych, tj.: informatyzacja urzędów, e-administracja i e-społeczeństwo. Krytyczne podejście do zaprezentowanych w planie założeń stało się jednak przeszkodą do jego przyjęcia. W rezultacie opracowano udoskonaloną, zaktualizowaną wersję – Program Zintegrowanej Informatyzacji Państwa (PZIP)[22]. Celem strategicznym nowego dokumentu programowego ma być zwiększenie wolumenu wysokiej jakości publicznych usług elektronicznych w Polsce. Za wyznacznik realizacji powyższego celu przyjęto odsetek osób (indywidualnych i przedsiębiorców) korzystających z powyższych usług. W opinii autorów

[20] Perkowski B., *Elektroniczny dowód osobisty jako element informatyzacji służby zdrowia*. Studia Oeconomica Posnaniensia 2013, vol. 1, no. 2 (251): 133-151

[21] Smoktunowicz U., *Plan Informatyzacji Państwa na lata 2011-2015*. Źródło internetowe: https://www.crn.pl/rynek/plan-informatyzacji-panstwa-na-lata-2011-2013-2015, data dostępu: 06.05.2017

[22] Program Zintegrowanej Informatyzacji Państwa. Ministerstwo Cyfryzacji, Warszawa 2016. Źródło internetowe: https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, data dostępu: 06.05.2017

dokumentu sposobem na osiągnięcie celu strategicznego powinno być zapewnienie interoperacyjności istniejących oraz nowych systemów informatycznych administracji publicznej m.in. poprzez eliminację zjawiska redundancji w zakresie ich funkcjonalności. Takie podejście ma prowadzić do budowy spójnego Systemu Informacyjnego Państwa dostarczającego kluczowych dla obywateli usług w sposób efektywny[23].

Obecny poziom dostępności usług cyfrowych w Polsce pozostaje niewystarczający zarówno pod względem potrzeb informacyjnych obywateli, jak również w kontekście możliwości oferowanych przez współczesne rozwiązania teleinformatyczne. Spośród najważniejszych przyczyn takiego stanu rzeczy istotną rolę odgrywają ograniczenia w zakresie wykorzystywania obecnych metod identyfikacji elektronicznej i uwierzytelnienia w systemach publicznych udostępniających cyfrowe usługi publiczne. W dobie dynamicznego rozwoju sektora usług dostępnych *on-line* możliwość przeprowadzenia identyfikacji elektronicznej i uwierzytelnienia staje się konieczna w celu zapewnienia użytkownikom bezpiecznego korzystania z różnego rodzaju aplikacji cyfrowych. Aktualnie identyfikacji elektronicznej oraz uwierzytelnienia w systemach informatycznych administracji publicznej dokonuje się na dwa sposoby: za pomocą mechanizmów funkcjonujących w instytucji administracyjnej (tj. własnych systemów informatycznych organizacji) lub poprzez mechanizm profilu zaufanego ePUAP[24]. Wymóg powszechności w odniesieniu do środków identyfikacji elektronicznej spełnia obecnie wyłącznie profil zaufany ePUAP, jednak jego dostępność i skala zastosowania nadal jest ograniczona. Szacuje się, że liczba użytkowników posiadających i korzystających z własnego profilu zaufanego ePUAP wynosi w skali całego kraju jedynie ok. 700 tys. osób[25]. Zasadniczo nie zmieniły tego faktu korekty wprowadzone w ostatnim kwartale 2016 roku dopuszczające możliwość potwierdzenia i autoryzacji profilu zaufanego ePUAP m.in. za pomocą systemu poświadczeń bankowych. Tym samym ograniczone wykorzystanie profilu zaufanego ePUAP wymusza kontynuację dalszego finansowania wewnętrznych

[23] MAiC 2012, Państwo 2.0 – Nowy start dla e-administracji, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.

[24] Uzasadnienie ustawy o zmianie ustawy o usługach zaufania. Źródło internetowe: https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, data dostępu: 06.05.2017

[25] Projekt ustawy o zmianie ustawy usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, Ministerstwo Cyfryzacji, 2017.

systemów identyfikujących użytkowników oddzielnie u każdego usługodawcy. Powstaje zatem dość paradoksalna sytuacja, w której istnieje rozwiązanie spełniające kryterium powszechnego środka identyfikacji elektronicznej, lecz przez jego niewystarczające upowszechnienie w społeczeństwie pojawia się konieczność rozwijania autonomicznych, rozproszonych narzędzi identyfikacyjnych w organach administracji publicznej, w których planowana cyfryzacja usług *de facto* uwarunkowana jest możliwością funkcjonowania powszechnej identyfikacji elektronicznej i uwierzytelnia usługobiorców organów administracyjnych.

Konsekwencją takiej sytuacji jest konieczność udostępnienia i przydzielenia poszczególnym użytkownikom odpowiednich uprawnień (tj. założenie indywidualnego konta) w systemie świadczącym określonego rodzaju usługi. Taki wymóg wiąże się z dodatkowymi trudnościami po stronie użytkowników obecnych systemów identyfikacji elektronicznej – sprawia, że osoba korzystająca z usług cyfrowych świadczonych przez różne podmioty musi nauczyć się i zapamiętać różne sposoby identyfikowania się w różnych systemach zarządzanych przez różnych dostawców usług. Taka niedogodność wynika z braku jednej, spójnej polityki bezpieczeństwa w systemach informatycznych dostawców usług cyfrowych, która w szczegółowy sposób regulowałaby zasady udostępniania i eksploatacji haseł (w zakresie np. wymaganej długości hasła, ilości znaków alfanumerycznych, etc.). Funkcjonowanie wielu różnych systemów identyfikacji elektronicznej staje się tym samym dla użytkownika praktycznym problemem. Co więcej, sposób i zakres identyfikacji elektronicznej w każdej instytucji jest uzależniony od zakresu i rodzaju usługi, którą identyfikacja ma zabezpieczać przed np. nieautoryzowanym przejęciem lub posługiwaniem się fałszywą tożsamością. Z perspektywy merytorycznej ma to swoje uzasadnienie: poziomy bezpieczeństwa powinny być bowiem różnicowane w zależności od statusu przetwarzanych w systemie informacji, a także od profilu realizowanej usługi. W rezultacie dochodzi do jeszcze większej atomizacji skali rozproszenia identyfikacji elektronicznej i uwierzytelnienia w dążącym do deklarowanej spójności systemie informacyjnym państwa.

W związku z powyższymi niedogodnościami powstaje pytanie, w jaki sposób zreorganizować uciążliwy i skomplikowany dotychczasowy system identyfikacji elektronicznej i uwierzytelniania czyniąc go bardziej dogodnym przede wszystkim dla obywatela? Z perspektywy użytkowników obecnych systemów identyfikacji elektronicznej optymalnym rozwiązaniem byłaby możliwość posługiwania się podobnym (lub identycznym) zestawem danych identyfikujących w ramach różnych usług. Wprowadzenie powyższej zasady

elastyczności powinno nastąpić w środowisku systemów identyfikacyjnych budzących zaufanie użytkowników do korzystania z aplikacji cyfrowych na zdecydowanie większą, niż dotychczas, skalę. Pomocną w tym aspekcie może okazać się świadomość informacyjna naszego społeczeństwa budowana na doświadczeniu korzystania z komercyjnych usług cyfrowych dość powszechnie udostępnianych przez podmioty sektora bankowego, telekomunikacyjnego i - w niektórych przypadkach - także zdrowotnego. Wydaje się, że kompetentne działania informacyjne odwołujące się do znanych i wykorzystywanych na co dzień przez większość obywateli mechanizmów identyfikacji elektronicznej i uwierzytelnienia w obszarze np. bankowości elektronicznej czy usług telekomunikacyjnych mogłyby być dobrym punktem wyjścia w kierunku znacznie większego, niż do tej pory, korzystania z cyfrowych usług administracji publicznej.

Tak znaczące uproszczenie sposobu identyfikacji elektronicznej i uwierzytelnienia obywateli będzie korzystne także dla organów administracji publicznej udostępniających usługi cyfrowe – jeśli będą mogły opierać swoje działania na funkcjonalnym, wiarygodnym systemie identyfikacji elektronicznej i uwierzytelnienia zarządzanie dotychczasowymi własnymi systemami identyfikacyjnymi pełniącymi te same funkcje nie będzie konieczne. W celu zrównoważonego wprowadzania omawianych rozwiązań zmierzających do zagwarantowania powszechności stosowania i bezpieczeństwa użytkowania środków elektronicznej identyfikacji i uwierzytelnienia w naszym społeczeństwie zaproponowano usankcjonowanie na poziomie ustawowym następujących praw, obowiązków oraz celów przewidzianych dla podmiotów podlegających identyfikacji[26]:

- szybkie osiągnięcie znacznej liczby użytkowników posługujących się środkami identyfikacji elektronicznej, co dodatkowo będzie sprzyjać budowie i udostępnianiu nowych usług cyfrowych;
- rozwój niezawodnej oraz otwartej na sektor prywatny i innowację architektury zapewniającej identyfikację elektroniczną, która to przyczyni się do pozytywnego wizerunku e-administracji;

[26] Uzasadnienie ustawy o zmianie ustawy o usługach zaufania. Źródło internetowe: https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, data dostępu: 06.05.2017

- zapewnienie odpowiedniej dywersyfikacji środków identyfikacji elektronicznej ze szczególnym naciskiem na zapewnienie publicznych - udostępnionych przez Państwo, środków identyfikacji elektronicznej na wszystkich poziomach bezpieczeństwa przy jednoczesnej klarowności systemu i oferowanych przez niego metod identyfikacji dla obywateli;
- popularyzacja środków identyfikacji elektronicznej, które zapewnią powszechny dostęp do istniejących usług cyfrowych administracji publicznej;
- zapewnienie wysokiej elastyczności i potencjału wzrostu dla rynku usług cyfrowych administracji publicznej i komercyjnych;
- zapewnienie wysokiego poziomu bezpieczeństwa danych obywateli.

Podsumowanie

Projekt ustawy o zmianie ustawy usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw z kwietnia bieżącego roku przygotowany przez Ministerstwo Cyfryzacji przyjmuje za cel wdrożenie sprawnie funkcjonującej elektronicznej identyfikacji w Polsce w oparciu o powszechnie dostępne, przejrzyste i bezpieczne rozwiązania organizacyjno-techniczne. Zgodnie z przedstawionymi w projekcie założeniami rozwiązania te mają zapewniać możliwości użycia w publicznych usługach *on-line* środków identyfikacji elektronicznej wydawanych przez różne podmioty, w tym także wykorzystanie już istniejących środków identyfikacji elektronicznej stosowanych w usługach *on-line* świadczonych przez podmioty prywatne (np. banki, telekomy).

Dzięki takiemu pomysłowi ustawodawca zakłada szybkie pokonanie bariery braku powszechnego dostępu do środków identyfikacji elektronicznej. Przedstawione w projekcie założenia nakreślają również publiczny schemat identyfikacji elektronicznej o charakterze modelu rozproszonego (federacyjnego) funkcjonującego na bazie wielu środków identyfikacji elektronicznej. Mają być one wydawane przez różne podmioty, w tym także przez dostawców komercyjnych. Jego centralnym elementem ma być tzw. Krajowy Węzeł Identyfikacji Elektronicznej (KWIE) pełniący przede wszystkim funkcję koordynacyjną i pośredniczącą między węzłami komercyjnymi, węzłem transgranicznym, dostawcami usługi i dostawcami atrybutów.

Zakłada się, że KWIE zostanie zintegrowany z systemami informatycznymi udostępniającymi cyfrowe usługi publiczne oraz dostawcami środków identyfikacji elektronicznej w terminie do 31 grudnia 2017 r. Z kolei do końca przyszłego roku powinna nastąpić obowiązkowa migracja wszystkich portali zintegrowanych na dzień 31 stycznia 2017 r. z Profilem Zaufanym, zaś do 31 grudnia 2020 r. migracja portali posiadających własny system logowania.

Piśmiennictwo:

[1] Goc. M., Tomaszewski T., Lewandowski R., *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości,* Volumina, Warszawa 2016, s. 289
[2] Kawiński A., Sieradz A.[red.], *Wyzwania informatyki bankowej*: materiał przygotowany na podstawie seminariów IT w instytucjach finansowych organizowanych przez Gdańską Akademię Bankową Instytut Badań nad Gospodarką Rynkową, Gdańsk 2014
[3] Lewandowski R, Miękina A. *Certyfikacja w zakresie Common Criteria – wstępna koncepcja budowy polskiego modelu*. Człowiek i Dokumenty. 2015;39:35.
[4] Lewandowski R. *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA.* Journal of Health Policy, Insurance and Management – Polityka Zdrowotna. 2015;16:75–84
[5] Lewandowski R., *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, Polski Przegląd Nauk o Zdrowiu 3;(48): 2016
[6] Lewandowski R., *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna" 2015, nr 16, s. 77
[7] Lewandowski R., Karta Ubezpieczenia Zdrowotnego – zmiany. Źródło internetowe: https://serwiszoz.pl/zarzadzanie/karta-ubezpieczenia-zdrowotnego-zmiany-3170.html, data dostępu: 09.05.2017
[8] MAiC 2012, Państwo 2.0 – Nowy start dla e-administracji, Ministerstwo Administracji i Cyfryzacji, Warszawa 2012.
[9] Perkowski B., *Elektroniczny dowód osobisty jako element informatyzacji służby zdrowia*. Studia Oeconomica Posnaniensia 2013, vol. 1, no. 2 (251): 133-151
[10] Program Zintegrowanej Informatyzacji Państwa. Ministerstwo Cyfryzacji, Warszawa 2016. Źródło internetowe: https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, data dostępu: 06.05.2017
[11] Program Zintegrowanej Informatyzacji Państwa. Ministerstwo Cyfryzacji, Warszawa 2016. Źródło internetowe: https://mc.gov.pl/files/program_zintegrowanej_informatyzacji_panstwa_1.pdf, data dostępu: 06.05.2017

[12] Projekt ustawy o zmianie ustawy usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, Ministerstwo Cyfryzacji, 2017.
[13] Projekt ustawy o zmianie ustawy usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, Ministerstwo Cyfryzacji, 2017.
[14] Smoktunowicz U., *Plan Informatyzacji Państwa na lata 2011-2015*. Źródło internetowe: https://www.crn.pl/rynek/plan-informatyzacji-panstwa-na-lata-2011-2013-2015, data dostępu: 06.05.2017
[15] Uzasadnienie ustawy o zmianie ustawy o usługach zaufania. Źródło internetowe: https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, data dostępu: 06.05.2017
[16] Uzasadnienie ustawy o zmianie ustawy o usługach zaufania. Źródło internetowe: https://legislacja.rcl.gov.pl/docs//2/12297458/12427868/12427869/dokument284778.docx, data dostępu: 06.05.2017
[17] Wachnik D., *Rozporządzenie eIDAS - na pograniczu technologii i prawa*. Elektronika 2/2014: 42-44
[18] Źródło internetowe: https://www.buergerkarte.at/en/downloads-card.html, data dostępu: 19.05.2017
[19] Źródło internetowe: https://www.buergerkarte.at/en/pdf-signature-mobile.html, data dostępu: 19.05.2017
[20] Źródło internetowe: www.signature-verification.gv.at, data dostępu: 19.05.2017

Streszczenie

W artykule omówiono aktualne uwarunkowania implementacji usług identyfikacji elektronicznej i uwierzytelnienia za pomocą nowoczesnych technologii teleinformatycznych, które mają znaleźć zastosowanie w systemie opieki zdrowotnej. Ich wdrożenie stanowi zarazem krok milowy, jak również warunek zapewnienia rzeczywistego bezpieczeństwa informacyjnego dla pacjentów oraz pracowników sektora opieki zdrowotnej.